A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2002-0183-4C

INDEPENDENT STATE AUDITOR'S
REPORT ON INFORMATION TECHNOLOGY
AND FINANCIAL-RELATED CONTROLS
AT THE MASSACHUSETTS COLLEGE OF LIBERAL ARTS

JULY 1, 2000 THROUGH OCTOBER 30, 2001

OFFICIAL AUDIT REPORT

JANUARY 31, 2002

2001-0194-4C

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts College of Liberal Arts (MCLA), formally known as North Adams State College, was established in 1894 by Chapter 457 of the Acts of 1894. The College is governed by the Commonwealth's Board of Higher Education and is overseen by a board of trustees appointed by the Governor. The College has approximately 1,150 full-time students and 350 part-time students. The College is located in the northwest corner of Massachusetts, bordered by Vermont to the north and New York State to the west. MCLA was supported by a fiscal year 2001 budget of $27.4 million, of which $14.1 million was state appropriated, $10.4 million was from trust funds, and tuition and fees, and $2.9 million was from federal grants and loans.

MCLA is a public, four-year liberal arts college that offers degree programs in the arts and sciences, as well as a graduate degree program in education. The College's Division of Continuing Education also offers credit and non-credit courses.

The College's information technology resources are managed by three organizational groups: Computer Services (CS), Computer Support Services (CSS), and the Treasurer's Office. At the time of our audit, there were approximately 435 microcomputers campus wide for faculty, staff, and computer laboratories.

Computer Services (CS) provides systems for the College's administrative functions. It is comprised of six full-time staff members, including a Director who reports to the Vice President of Administration and Finance. CS operates and maintains an Alpha (digital) 4000 minicomputer and file servers which are located in a computer room environment. Mission-critical applications include the Student information System (SIS), Billing and Receivables (BR) application, financial aid management, and student registration. In addition, CS maintains applications for the College's inventory system, campus police ID card system, and a course evaluation system. The CS Department has a fiscal year 2001 budget of $414,197, including salaries.

The Student Information System (SIS), which operates on the Alpha 4000, contains all of a student's demographic and academic information. This includes enrollment and academic history, test scores, academic status, major/minor degree information and information for student billing. The other primary application, the Billing and Receivables application, serves as the College's primary financial accounting and business system. The BR is a centralized student

system that supports revenue collection by producing student bills and in recording and processing receipts.

MCLA's academic computing needs are managed by the Computer Support Services Department (CSS), which is comprised of five full-time and one part-time staff members, including a director who reports to the Vice President of Academic Affairs. The CSS supports faculty and students and academic functions by operating the College's computer labs, IT networks, e-mail, student user files, an alumni data base, and the College's website. CSS operations provide local area network (LAN), wide area network (WAN) and the Internet access for faculty, staff and students. Academic functions, along with the College's website are supported through the use of five file servers operating with Novell Windows NT, which is licensed for educational software applications. The five file servers host approximately 120 microcomputer workstations in six computer laboratories. The CSS fiscal year 2001 operating budget totaled $332,500, including staff salaries, and reflects a decrease of 20% from fiscal year 2000.

The MCLA's Treasurer's Office uses the Great Plains Accounting System to support the accounts payable function as well as the MMARS (Massachusetts Management Accounting and Recording System) and the Human Resources/Compensation Management System (HR/CMS) to support College administrative functions.

The Office of the State Auditor's examination focused on an evaluation of IT-related general controls over MCLA's computer operations and a review of certain financial-related operations.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

We performed an information technology (IT) and financial-related audit at Massachusetts College of Liberal Arts, covering the period July 1, 2000 to October 30, 2001. The audit was conducted from July 16, 2001 through October 30, 2001.

The scope of our IT-related audit included an evaluation of the administrative and academic IT functions. Areas reviewed included IT-related organization and management, physical security, environmental protection, system access security, authorized use of software, on-site and off-site storage of magnetic backup media, and disaster recovery and business continuity planning.

Regarding financial-related areas, we examined controls over IT-related service contracts and procurement and inventory record-keeping of IT-related assets.

Audit Objectives

Our primary audit objective regarding the examination of IT-related controls was to determine whether the College's administrative and academic IT environment was sufficiently controlled to support automated systems and to account for and safeguard IT-related assets. We sought to determine whether MCLA's internal control environment, including policies, procedures, practices, and organizational structures, provided reasonable assurance that IT-related control objectives would be achieved to support the College's business objectives and to prevent and detect related undesired events. Our audit objective regarding organization and management was to determine whether IT-related roles and responsibilities were clearly defined, points of accountability were established, appropriate organizational controls were in place, and that IT-related policies and procedures adequately addressed the areas under review. In conjunction with our review of the IT environment, we sought to determine whether MCLA had implemented written and approved policies and procedures regarding authorized access, safeguarding assets, and proper accounting for IT-related assets.

We sought to determine whether adequate physical security and environmental protection were in place over and within areas housing IT-related assets to provide reasonable assurance that access would be available to only authorized users and that damage to, or loss of, computer equipment, software, and data files would be prevented or detected. The areas reviewed were the College's administrative and academic data centers, including the MCLA Treasurer's file server

room, administrative offices, computer laboratories and the administrative off-site backup media storage location. A further objective was to evaluate whether adequate controls were in place to prevent and to detect unauthorized system access to the data files and software residing on MCLA's automated systems. Our examination of physical security and environmental protection for IT resources did not include academic offices.

We sought to determine whether adequate business continuity plans were in place to provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period should a disaster render the MCLA's computerized functions inoperable. In addition, we determined whether adequate on-site and off-site storage was being provided for backup copies of mission-critical and essential application software, data files, and archival copies of data files.

Regarding our examination of financial-related activities, a primary audit objective was to determine whether MCLA had implemented adequate inventory controls to provide reasonable assurance that all property and equipment, including computer equipment and software, were properly recorded in the College's inventory record, accounted for, and reported to the Office of the State Comptroller in accordance with laws and regulations. In addition, we determined whether adequate controls were in place and in effect to provide reasonable assurance that the purchasing, receipt, recording, and monitoring of IT-related assets were being properly performed. A further objective was to determine whether written contracts were in place to cover IT-related services and were properly signed and dated, whether incorporated vendors were properly registered with the Office of the Secretary of State, and whether services and deliverables were being provided to the College in accordance with the contracts.

Audit Methodology

To determine audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of relevant IT operations, reviewing and evaluating internal controls, and interviewing senior management to discuss MCLA's control environment. In conjunction with our review of the internal control environment, we determined whether MCLA had developed and implemented, reviewed and approved internal control documentation, including IT-related policies and procedures. In order to obtain a preliminary understanding of the MCLA's financial-related activities regarding IT-related contract administration and the safeguarding of, accounting for, and reporting of property and equipment, we interviewed College management and staff, reviewed relevant Commonwealth statutes and regulations

regarding fixed-asset management, and reviewed the College's related policies and procedures, selected contracts, and records.

Regarding our examination of organization and management, we interviewed senior management; obtained, reviewed, and analyzed existing IT-related policies, standards, procedures, and the IT strategic plan to determine their adequacy and assessed IT-related management practices. To determine whether an IT-related steering committee was in place and operating to help provide adequate oversight of IT functions and processes across the College, we interviewed senior management, and IT staff, and reviewed minutes of steering committee meetings. To determine whether MCLA's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technical knowledge requirements, we obtained a current list of the personnel employed by the Computer Services, Computer Support Services and the Treasurer's Office and the copy of IT-related job descriptions and job specifications and reviewed and compared the job descriptions and job specifications to current IT-related assignments and responsibilities.

To evaluate physical security, we interviewed senior management and security personnel, conducted walk-throughs of areas reviewed and obtained and reviewed forms designed to record security violations and incidents. We also obtained a list of employees who had keys to the College's data centers and, through observation, determined the adequacy of physical security controls for data center access, such as locks, physical access procedures, visitor logs, motion detectors and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were employees of the College. Further, to determine the adequacy of physical security controls regarding MCLA's microcomputer systems located throughout the College, we conducted site visits to office areas, computer labs, and on-site and off-site storage areas.

To determine whether IT resources were subject to adequate environmental protection, we conducted site visits to areas housing IT equipment and backup copies of software and data files. Our examination included a review of general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supplies, emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observation, and documentation reviews. To determine the adequacy of environmental controls, we conducted a walk-through and evaluated controls in place within the data center and selected areas and assessed the sufficiency of control-related policies and procedures.

To determine whether MCLA could account for all copies of application software residing on its stand-alone and networked workstations, we determined whether a software inventory record was available, evaluated control procedures, and interviewed MCLA management. In the absence of a software inventory record, to identify the nature and extent of software, we requested a list of software installed on MCLA's systems and reviewed related documentation, such as purchase orders and licenses for application software residing on the minicomputer and microcomputer systems. To determine whether appropriate controls were in place to prevent and detect the use of unauthorized software, we reviewed policies and procedures and interviewed IT management and staff. We were unable to determine whether only authorized software resided on automated systems because of the absence of sufficient records of software available for use and/or installed on the College's systems and a list of software authorized for use.

To determine whether adequate system access security controls were in effect, we reviewed and determined the appropriateness of related policies and procedures, assessed required security levels, determined whether security requirements had been established, reviewed procedures to activate and deactivate user privileges, reviewed logon ID and password administration and determined whether possible security violations were being detected, recorded, and corrected. We determined whether MCLA's system access security policies and procedures prevented and detected unauthorized access to application software and data files installed on the minicomputers and the client/server systems. To determine whether the administration of logon ID and password security was being properly carried out, we reviewed security procedures with the Director of the Computer Services Department, who was responsible for access administration to the mainframe and minicomputers systems.

Our tests of system access security included a review of access privileges for those staff members who were authorized to access the minicomputers and the client server systems. We determined whether logon ID and password access was established for authorized users and employees of the College. We determined the frequency with which all staff authorized to access the automated system were required to change their passwords. We compared the list of staff authorized to access the information systems with the current MCLA employee list to determine whether individuals authorized to access the systems were current employees. We also reviewed password administration controls, such as granting passwords, required length and composition of passwords, related security procedures, frequency of password changes and restrictions on using previously used passwords.

To assess the adequacy of business continuity planning, we reviewed disaster recovery and

business continuity planning procedures documented by the College for the administrative data center. We interviewed MCLA management to determine whether the criticality of application systems had been assessed and whether risks and exposures to the computer operations had been evaluated. We also reviewed the current status of formal business continuity planning for information technology. Further, we reviewed the adequacy of provisions for on-site and off-site storage of critical backup media and conducted site visits to the administrative computing backup media storage areas to assess the adequacy of physical security and environmental protection. We assessed the adequacy of inventory control procedures for backup copies of magnetic media.

To accomplish our review of financial-related controls, we reviewed contract-related policies and procedures and examined IT-related contracts and services for fiscal year 2000 and the first five months of fiscal year 2001. We interviewed management and obtained and reviewed copies of selected contracts to determine whether they were approved by appropriate parties and whether the proper signatures and dates were included in accordance with state requirements. We determined whether desired deliverables and services were provided. In addition, we determined whether vendors that were incorporated within, or outside of Massachusetts were properly registered with the Commonwealth's Office of the Secretary of State. as domestic or foreign (i.e., non-Massachusetts) corporations, respectively.

To determine whether adequate controls were in place and in effect to properly account for MCLA's IT-related property and equipment, we reviewed inventory control procedures for hardware and software. We determined whether computer equipment was properly tagged with state identification numbers and serial numbers and whether the serial numbers attached to the equipment were properly recorded on the hardware inventory list. To determine whether the records for hardware valued at $ 1,000 or greater, for fiscal year 2001, valued at $736,000 were current, accurate, complete, and valid, we chose for testing a judgmental sample of 118 out of 444 items of MCLA's computer equipment. We traced the state identification numbers of the hardware items listed on the inventory record to the actual equipment on hand. We judgmentally selected an additional 27 items of newly purchased computer equipment and traced the items to the inventory record. We confirmed purchase documentation for hardware purchased during fiscal year 2000 and valued at $52,903 to the inventory record and then to the equipment on hand.

We determined whether MCLA had complied with the annual GAAP reporting requirements, as promulgated by the Commonwealth's Office of the State Comptroller, by making its submission with complete and valid fixed-asset information and supporting financial documentation doing so in a timely manner.

The audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and industry auditing standards.

AUDIT SUMMARY

Based on the results of our audit, internal controls in place at Massachusetts College of Liberal Arts provide reasonable assurance that control objectives related to on-site and off-site storage of backup media, and physical security and environmental protection over IT resources would be met. We determined that procedures regarding the generation of and on-site and off-site storage of backup copies of magnetic media were adequate. In addition, we found that adequate physical security and environmental protection controls were in place for the College's data processing environment, including office areas and computer labs. However, our audit revealed that controls needed to be implemented or strengthened in the areas of IT-related organization and management, logical access security, hardware and software inventory, and disaster recovery and business continuity planning for information technology.

We found that internal controls needed to be strengthened with respect to IT organization and management. Although IT responsibilities appear to be well understood and points of accountability were generally well established, IT management control practices needed to be strengthened to provide enterprise-based oversight and IT strategic planning, and enhance IT policies and procedures. At the time of our audit, we found a general absence of documented IT strategic and tactical plans covering the College's overall IT environment. Specifically, we found that the College did not have an IT steering committee in place to provide management guidance and oversight. We encourage the College to conduct a detailed survey and analysis of IT requirements, and to strengthen and formalize an IT planning process that will yield strategic and tactical IT plans to support the College's mission. Although there was a degree of oversight in place, it was focused more toward the responsibilities of each of the three IT functional areas then the College at large. We believe that the development of an IT steering committee is critical to the College with respect to long-term issues, specifically strengthening oversight for strategic planning, configuration management, and infrastructure planning. In addition, we found that certain job descriptions needed to be updated to more accurately reflect current IT-related employee responsibilities.

Our review of system access security for the Student Information System (SIS) that supports administrative operations indicated that access security administration needed to be strengthened. We found that although procedures were in place to authorize and activate access privileges and to periodically change passwords, procedures needed to be strengthened to ensure timely deactivation of access privileges no longer authorized or needed. We found that the security

administrator was not consistently being notified in a timely manner of changes in employment status of users having access to automated systems by department heads or the MCLA's Human Resources Department. Our tests of authorized users of the SIS system revealed that at the time of our test, three out of sixty-five user accounts were active for individuals no longer employed by the College. We recommend that the College require that department heads, deans, and MCLA's Human Resources Department promptly notify the security administrator of changes in employee status that could warrant temporary or full deactivation of user access privileges.

Our examination of inventory control revealed that the College's Treasurer maintained a master inventory as a system of record to account for property and equipment. In addition, the College had documented policies and procedures regarding inventory control. Based on our examination, we found that increased effort was needed to ensure that hardware and software are properly accounted for. Audit test results drawn from a sample of IT-related items, each valued at $1,000 or more, indicated that although most items were properly identified and all IT resources tested were tagged, there were a number of instances where the location of the items as designated on the inventory record was incorrect. Based on a judgmental sample of 66 IT-related items from the fixed-asset inventory, we found that 25 (38%) out of 66 IT-related items could not be readily located from the master inventory record. Second, based on another sample of IT resources selected from their physical locations in office areas and traced back to the inventory list, we found that 19 (37%) items out of 52 items of computer equipment tested could not be identified on the master inventory record.

Regarding software, we found that adequate controls were not in place to ensure that software products residing on microcomputers were properly accounted for or that unauthorized use or copying of software would be detected. Documented policies and procedures, if followed, would provide reasonable assurance that the use of only unauthorized software would be prevented. Our review indicated that detective controls needed to be implemented or strengthened to confirm the use of authorized software and to detect the use of unauthorized software. Establishment of a software inventory record for the academic and administrative IT departments would provide a base of comparison for periodic checks of installed software to determine whether only authorized software was installed. The College should consider using LAN-based software to identify the software packages installed on file servers and networked workstations. During the course of our audit, nothing came to our attention to indicate that unauthorized or illegal copies of software were installed on College systems.

Although we determined that procedures regarding the generation of backup copies of

magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. We found that there was a general absence of documented plans to address disaster recovery and business continuity for automated operations. Our audit disclosed that the College did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for administrative and academic functions could be regained effectively and in a timely manner, should a disaster render automated systems inoperable. Although we found that the College had begun to formulate a business continuity strategy, an alternate site contingency plan had not yet been developed nor had user area plans been established to document the procedures required to regain business operations in the event of a disaster.

Our review of the College's IT-related service contracts revealed that all contracts were properly signed and approved and that services were delivered. In addition, all vendors incorporated as either a foreign or domestic corporation were found to be properly registered with the Commonwealth's Office of the Secretary of State.

AUDIT RESULTS

1. Hardware and Software Inventory

Our review of IT-related hardware inventory revealed that controls needed to be strengthened to provide for the proper accounting of these assets. We found that there were three inventory records of computer hardware being maintained at MCLA. The master inventory record was being maintained by the College's Treasurer as a system of record, while the other inventory records were being maintained by the Computer Services Department and the Computer Service Support Department to assist in managing IT resources across the College. We determined that the three inventories had not been reconciled to help ensure the integrity of inventory records. We also determined that an annual physical inventory was not being performed to assist in verifying the master inventory record.

Our inventory tests conducted against the master inventory record indicated that not all of the identified locations were correct. The 118 items we tested represented 25% of all IT items on campus that were valued at $1,000 or more. The total stated value of IT resources, each of a stated value of $1,000 or more totaled $736,695. We examined the inventory record from two perspectives: from the inventory list we selected a sample and determined whether the assets were located in the office or lab area designated on the inventory list, and if located, whether the inventory list accurately reflected identifiable information. Our audit disclosed that 25 (38%) from our first sample of 66 IT-related items of the fixed assets within our judgmental sample could not be readily located from the master inventory record. Second, based on another sample of items selected from College office areas, we found that 19 (37%) items from a sample of 52 items of computer equipment tested could not be identified on the master inventory record.

It came to our attention that all purchases of computer equipment made in fiscal year 2001 were not included in the master inventory record. A test performed on a sample of IT-related purchases from the fiscal year 2001 indicated that out of a total of $54,593 worth of items tested, $ 26,988 was not recorded on the master inventory record. The College had expended a total of $159,459 in fiscal year 2001 on IT equipment.

At the time of our review of software inventory controls, management could not provide a software inventory record. Because of the lack of an up-to-date, accurate, and complete record of software inventory, the College could neither account for all copies of software installed on the LAN and microcomputers nor determine whether only authorized software was residing on their systems. In addition, the absence of a software inventory record precluded an accounting of the

total number of software copies allowed per the various software license agreements.

Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and software and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record. In addition, prudent business practices advocate that the software inventory record be used to help prevent unnecessary software expenditures and to detect theft, unauthorized installation of software, and potential software copyright infringements.

Reconciliation of software inventory records to software residing on computers would provide a detective control to identify misplaced, lost, stolen, unauthorized, or potentially illegal copies of software. Asset control is facilitated when all software is properly identified, indicating the computer on which it resides.

State law requires complete and accurate inventory records of state-owned assets. In accordance with MGL, Chapter 7, Subsection 4A, each state agency is required to record and report state-owned assets to control agencies, such as the Office of the State Comptroller (OSC). Our audit confirmed that the College had submitted a GAAP report indicating total values for hardware and software.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989 states, in part, that "the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts."

Shortcomings in inventory control were the result of a lack of both management attention and proper assignment of asset control responsibilities. In addition, the absence of an accurate inventory record for software may also hinder the College's ability to determine whether unauthorized and/or illegal software had been installed on microcomputer workstations. Otherwise, undetected copyright infringements regarding potentially illegal software copies could place the College at risk of possible legal action.

Recommendation:

The College should enhance controls over its record-keeping to provide for maintenance of a perpetual hardware and software inventory record. Specifically, we recommend that policies and procedures be enhanced to require that a perpetual hardware and software inventory record be

maintained and be periodically verified through appropriate inventory reconciliation controls, such as testing to physical hardware and the software packages installed on file servers and other computer equipment. We recommend control procedures be implemented to ensure that all IT procurements that are accepted are included on the inventory record. We recommend that the College use their Property Change Forms as source documents to identify relocations of equipment. The inventory record should reflect any changes to computer hardware and software packages installed or available for installation.

We recommend that the College consider using their established system of record for property and equipment to include software. Software inventory records should include pertinent information, such as the name of the software product, acquisition date and source, cost, version number, number of copies of software acquired and allowed, and the IT configuration or platform upon which the software has been loaded.

We recommend that the College consider using a single inventory system to address asset accounting, reporting, and configuration management objectives. In addition to having the system record identifiable information on IT resources, data files could include information to support IT configuration management plans, such as status of equipment and its relative importance to mission-critical systems.

We recommend that MCLA management ensure that adequate direction and resources are available to support a perpetual inventory of all IT-related equipment and software.

Auditee Response:

> *Massachusetts College of Liberal Arts acknowledges that improvements need to be made in our inventory control. However, at the time that the State IT auditors arrived on campus, July 2001, MCLA was in the process of moving to a new accounting package with a fixed-assets module. Our implementation of the new module had just begun at the time the auditors had arrived on campus. Consequently, the reconciliation of inventory items was based on an incomplete system.*
>
> *The College believes that once all inventory information is transferred to the new Great Plains Software Package Fixed Asset System, we will have in place the appropriate software to maintain and periodically verify inventory. It was unfortunate that the system was being implemented at the time that the auditors started on campus, but we believe this new system appropriately handles our fixed asset needs.*
>
> *The College does have control procedures in place to ensure that all IT procurements are recorded on the inventory record. The College has asked the audit team for the 19 specific items, totaling $26,988.00, that were alleged to not*

be recorded during Fiscal Year 2001 as new IT purchases. It is the College's belief that controls are in place to record the procurement of all IT purchases. Absent the specific detail of what was missing, the College cannot reconcile its accounts against that of the auditors.

The College received the list identifying these specific items with a draft copy of the audit report. In addition to making sure all items were on the master inventory, we confirmed their location on campus. Consequently, all of these newly purchased items are appropriately entered into the master inventory system with confirmed locations.

The College has in place Property Change Forms as well as an established procedure utilizing e-mail, i.e., when property, particularly IT items, are moved from one office to another. We feel that once all inventory records have been moved to the new Fixed Asset System we will be better able to enforce the College policy which requires a completion of a form when IT property is moved.

In this past year, several offices have moved in anticipation of a major building renovation. We believe that this disruption to our normal operation contributed to the problems addressed in this recommendation.

With a draft copy of the audit report, the College received a list identifying 25 specific items that were not readily located at the time of the audit. From this list, 22 items have been located. Of the remaining three items, two have been cannibalized to repair other machines and one was discarded. The College is reviewing its procedure to manage these specific actions in the future.

The College agrees that software with a value of greater than $1,000 will be placed on our fixed asset inventory.

The College faces several issues in going to a single inventory system to address asset accounting, reporting and configuration management objectives. Our fixed asset system is designed to track all inventory items, including IT equipment as such. It is important that this system track assets for institutional investments for accounting reasons. The inventory system maintained by the Computer Services Department is designed to track configuration management plans, status of equipment, and software and hardware issues. We believe that it is essential to have two separate systems as they are managed because the information managed is quite different. However, we underscore the importance of reconciling the systems to each other on a periodic basis for control reasons.

In addition, MCLA has purchased automated software that will use the LAN to inventory both hardware and software assets. Arrangements for checking the information discovered and tracked by this software against perpetual inventory records kept by the fixed asset inventory system will be finalized once both systems are fully operational.

The College agrees that adequate direction and resources need to be made available to support a perpetual inventory of all IT-related equipment and

software. We believe that the College has the appropriate tools and human resources to do this.

Auditor's Reply:

We are pleased that the College is moving to an automated fixed-asset inventory system and recognizes that adequate resources are needed to support a perpetual inventory of all IT-related equipment and software. With respect to the recording of IT items purchased in fiscal year 2001, we acknowledge the College's statement that the 19 items, totaling $26,988, that were not recorded on the inventory as of June 30, 2001 are now fully recorded and their locations have been verified by the College.

We acknowledge that the College has a Property Change Form to record changes in location when IT items are moved within the campus, but believe that the forms should be used regardless of status of the migration of inventory data to the new Great Plains Software Package Fixed Asset System.

We agree that there are two distinct uses of inventory-related information; one for asset accounting and the other for configuration management. Our suggestion is for future consideration where movement toward integrated inventory related sub-systems benefiting from a single database management system would replace entirely separate systems. Understandably, since the College is positioned to use the two systems for the time being, we recommend that appropriate reconciliation be performed to help ensure an adequate level of data integrity. We agree with the College's procurement of LAN-based software to inventory hardware and software.

2. System Access Security

Our audit revealed that system access security over MCLA's local area network and microcomputer systems needed to be strengthened to ensure that only authorized users have access to the systems. We found that although adequate procedures were being followed to authorize and activate user privileges to the College's automated systems, controls regarding timely deactivation of user accounts needed to be strengthened.

We found that there were written policies and procedures in place requiring that the Computer Service Department be informed when an employee terminates employment at the College. However, written notification was not consistently being given from the College's Human Resources Department, department heads, or deans informing the Computer Service

Department of changes in employee status (e.g., terminations, leaves of absences, or transfers) that would necessitate deactivation of user accounts. Our tests of access security for the administrative LAN indicated that, contrary to sound access-security practices, sufficient documentary evidence was not available to indicate timely notification to the Computer Services Department and subsequent deactivation of user accounts. Our tests disclosed that there were active user IDs and passwords for three individuals who were no longer employed by the College. Our tests of the Student Information System application indicated that three out of sixty-five users were not listed on the May 2001 official employee record.

Our audit disclosed that although College could provide information as to the last date of use of user access accounts for the former employees still having active user privileges, information could not be provided as to when the user accounts were deactivated, or placed into "disuser" status. The audit test indicated that of the three users having active user privileges had not been employed at the College for up to one to two years. Our audit disclosed that although MCLA's Computer Use Policy documented security controls for logical access security to the LAN and microcomputers, the policy did not suffiently document the security controls for password deactivation procedures. The failure to deactivate user accounts in a timely manner places the College at risk to unauthorized use of established privileges (using another individual's user account having higher access privileges) or to unauthorized access.

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform basis. In addition, considerations of need-to-protect should be applied to data elements when data ownership is assigned and security requirements are being established. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact their level of authorization. For example, Human Resources should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access. Our review indicated that there was evidence of initial authorization, but that procedures were not in place to inform the security administration of changes in employment status. As a result, critical information on the College's systems may have been vulnerable to unauthorized access, alterations, and deletions.

The Commonwealth of Massachusetts' Internal Control Guide for Departments promulgated by the Office of the State Comptroller states in part ". . . an employee's password should be changed or deleted immediately upon notice of his/her termination, transfer, or change in responsibity." In addition, computer industry standards advocate that policies and procedures for

system access security be documented and approved to provide a basis for security administration and proper protection of information assets. The policies and procedures should address authorization for system users, establishing and activating user IDs and passwords, authentication of users, establishment of audit trails, notification of changes in user status, frequency of password changes, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access. The policies and procedures should also address emergency access guidelines for mission-critical applications to ensure that under emergency or disaster recovery situations, only authorized access is granted.

Formal policies and procedures for system access security should be in place that address password administration, activation and deactivation of access privileges, and monitoring of system access. The failure to develop written system access security policies and procedures and implement adequate controls places critical user files at risk to unauthorized access, modification, or loss.

Recommendation:

We recommend that procedures be established requiring written notification from the College's Human Resources Department and department heads of changes in personnel status (leaves of absence, changes in responsibilities, and terminations of employment) to the security administrator to help ensure timely modification or deactivation of access privileges. We recommend that the security administrator review, on a periodic or cyclical basis, with department heads the individuals authorized to access automated systems and verify that their access privileges are appropriate to their job responsibilities.

Auditee Response:

> *The College recognizes and acknowledges that procedures must be established requiring written notification from the College's Human Resources Department when changes in personnel occur requiring changes to the data use responsibilities of that user (termination, resignation, transfer). MCLA will develop such a policy and procedure. Also, we will review user security profiles periodically with Department Heads to make sure that security access, as noted, is appropriate.*
>
> *In acknowledging that there were three active accounts found during the time of the audit, the College has provided information to show that in all cases the former employee's last login was prior to their last employment date.*

Auditor's Reply:

We are pleased that the College will be developing formal procedures requiring written notification between the College's Human Resources Department and the Department heads when there is a change in an employees status that requires changes in access to the College's automated systems to support timely modification or deactivation of user access privileges. We recommend that notification to Computer Services and subsequent modification or deactivation of user privileges be documented and that an appropriate reporting mechanism be established. Since final responsibility for data integrity and security rests with user departments, we suggest that Computer Services provide department heads with timely notification of actions taken pertaining to their departments regarding modification or deactivation of user privileges.

3. Disaster Recovery and Business Continuity Planning For Information Technology

MCLA did not have a formal disaster recovery and business continuity plan to provide reasonable assurance that critical data processing operations for administrative and academic functions could be regained effectively and in a timely manner, should a disaster render automated systems inoperable. Although backup copies of critical and essential software and data were being made, specific arrangements had not been made to provide for alternate-site processing. In this regard, we found that there was no agreement in place with another organization for alternate-site processing should the LAN be unusable or inaccessible. Further, the College had not assessed the relative criticality of their automated systems to determine the extent of potential risks and exposure to data processing operations. Our audit also revealed that system users had not developed user-area contingency plans to address a potential loss of their automated processing.

Without adequate disaster recovery and contingency planning, including required user-area plans, the College was at risk of severely degraded or failed processing should automated capabilities be disrupted or lost. A loss of processing capabilities could adversely affect all administrative and academic functions supported by the data centers. Depending on when a disaster occurred during the academic year, the impact could hamper the College's ability to function. Furthermore, the absence of a comprehensive and tested disaster recovery plan could result in unnecessary costs, significant processing delays and loss of good will by students and faculty.

Disaster recovery and business continuity plans should be well tested to reduce time and the

risk of errors and omissions when restoring computer operations. An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility and, accordingly, the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate the need for a comprehensive and effective backup and disaster recovery and business continuity plan. Contingency planning should be viewed as a process to be incorporated with the functions of the organization, rather than as a project with successful completion upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans.

Recommendation:

The College should assess the criticality of automated systems to identify application priorities and critical resources. An analysis should be conducted to identify risks and exposures relating to the College's data processing operations and microcomputer environment. The College should identify potential processing alternatives and resources to be utilized should a disaster disrupt its data processing or business operations. Based upon these results, and input solicited from management and user departments, a written disaster recovery and business continuity plan should be developed, reviewed, and tested, to the extent possible; approved by senior management; and implemented.

We further recommend that procedures be developed to ensure that the criticality of systems is periodically reassessed, that the impact of changes in user needs or automated systems is evaluated, and that staff are adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, and complete. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel, and a

complete copy of the plan should be stored in a secure off-site location.

Auditee Response:

The College acknowledges its need to assess the criticality of automated systems and to identify application priorities and critical resources for business continuity plans. During the time of the audit, on October 15, 2001, a memo was distributed from the Office of the Vice President of Administration and Finance to begin work on such plan. It is the intention of the College to complete a draft business contingency plan by the end of the current academic year and to assess the viability of such plan over the summer of 2002.

It is our intention to have two approaches to business continuity planning. The first approach will be for events that affect the normal operation of campus as a teaching/learning institution, and the second will be for business continuity in the respective offices such as the Bursar's Office, Registrar's Office and the Admissions Office. With respect to the audit findings, the business contingency planning for the offices noted above will start with backup protocols to keep offices functioning with the loss of the Student Information System. It is essential that the normal functions of each office be maintained should service for data processing be disrupted.

The College acknowledges the importance of periodically reassessing disaster recovery and business continuity planning annually or in the event of a major system change.

Auditor's Reply:

We are pleased that the College acknowledges the need to assess the criticality of automated systems and will be taking steps toward developing a business continuity strategy for the College. Part of the value in assessing the relative importance of technology to business and academic areas will allow the College to triage their recovery and contingency planning efforts focusing first on high priority mission-critical systems and technology. As we would expect, we urge the College to extend its business continuity planning to automated systems and technology categorized as "essential" to the College's operations. We encourage the College to develop a comprehensive business continuity plan for all required administrative and academic applications. We strongly recommend user department participation in the development and testing of business continuity plans as well as that of the Computer Services and the Computer Support Services departments. Since business continuity planning requires that recovery and contingency plans be maintained, we recommend that responsibilities for maintaining the plans be assigned and that appropriate change control procedures be implemented to ensure that viable, authorized plans are in effect.

4. Information Technology Organization and Management

Although our audit revealed that MCLA had certain IT-related general controls in place, controls needed to be strengthened to ensure that IT and non-IT personnel performing IT-related functions had sufficient guidance to exercise their responsibilities in an effective and efficient manner. Although the College had documented IT-related policies and procedures, they were not uniformly applied across the College at large. In addition, certain policies and procedures needed to be enhanced to provide increased "rules of the road" and procedural guidance in the areas of inventory control, deactivation of user access privileges, IT strategic planning, and business continuity planning.

At the time of the audit, the College did not have a documented IT strategic plan to address IT management from an enterprise-based perspective. In addition, there was little evidence of detailed tactical, or operational, plans for IT functions. There was a general absence of documented and approved policies for IT strategic planning requiring the IT be aligned with organizational initiatives to support the mission of the College and to serve as a good basis upon which tactical plans could be developed. In addition, we noted that there was no documented evidence that IT strategic planning meetings had taken place. Although certain control procedures were being performed, the lack of an overall IT strategic plan inhibits the College's ability to ensure that the IT-related resources are being used in an effective and efficient manner and the IT governance objectives are being met.

Strategic planning is an essential tool that supports an entity's accountability in the allocation of limited resources. The lack of a comprehensive strategic plan increases the risk that future major system developments or IT-related acquisitions would not achieve management or user expectations and would be negatively impacted by time and budget over-runs. In addition, without a comprehensive strategic plan, analysis on development processes may vary substantially between projects, potentially resulting in information systems that are inefficient, are incompatible, and/or suffer increase cost for development and or system maintenance.

At the time of our audit, we determined that the College had recently divided its IT operations among three business units. Although we found that each area, i.e., the Treasurer, the Computer Services and Computer Support Services, was subject to management oversight, there was no one mechanism, or central point of accountability and oversight for IT resource management from an enterprise-based perspective. For example, the College did not have an overall IT steering committee in place to provide high-level management control and oversight. The College's IT

operations should be strengthened by detailing a more comprehensive technological direction necessary to support the MCLA's business functions. In addition, our audit indicated that the IT organizational structure, although reflecting an appropriate division of responsibilities and reporting lines, may not be sufficiently effective to accomplish the mission and goals of the College.

We found that the MCLA had documented job descriptions for all IT positions. However, we found that management needed to update certain job descriptions to accurately reflect actual employee responsibilities.

Recommendation:

We recommend that documented policies and procedures covering IT-related functions be enhanced to address operational and control objectives for IT inventory control, deactivation of access security privileges, IT strategic planning, and business continuity planning. We recommend that an analysis of IT-related functions be conducted to identify the organizational units within the College that perform IT-related functions. The latter should cover IT and non-IT functional units and should identify the job functions performed by multiple organizational units as well as functions performed only by a single department or unit. Understandably, the degree of complexity and decentralization will impact the requirements for standardization and procedural guidance. We recommend that the analysis determine whether the responsibilities for all IT-related job functions are clearly defined and assigned, and that appropriate points of accountability are in place.

We recommend that MCLA management establish an IT steering committee in order to provide sufficient formal guidance and enterprise-based oversight to support IT operations. With respect to IT strategic planning, we recommend that MCLA enhance their overall strategic planning framework to include IT strategic planning. We recommend that the College develop comprehensive IT strategic plans and tactical plans as part of its overall planning process.

Auditee Response:

> *The College acknowledges the need for documented policies and procedures covering IT-related functions. We also understand that these policies and procedures include IT inventory control, deactivation of access security privileges, IT strategic planning and business continuity planning. In developing such policies, the College reserves the right to decide on its organizational structure for efficient and effective management. A decision was made five years ago to create two separate entities to manage our computer environment. These include our computer support services and our computer services departments. Both have distinctly*

separate functions in service to our campus community, but we understand that both share responsibilities for secure access to College systems and data.

In the creation of appropriate policies and procedures as noted above, the College will be mindful of the interaction between our two computer departments and make sure that our approach to data security and integrity is maintained by both departments as they now stand. The College also agrees to consult the COBIT framework guidelines established by IT Governance Institute as a guide for establishing policies that are Enterprise based but Information Technology sensitive.

Lastly, we will do the appropriate analysis to determine that the responsibilities for all IT-related job functions are clearly defined and assigned and that appropriate points of accountability are in place.

The College agrees to establish an IT steering committee to provide formal guidance and enterprise-based oversight for IT operations on campus. In doing so, however, it is important to acknowledge that information technology planning has been a part of the College's overall strategic planning.

Since 1994, various committees have existed on campus to oversee IT-related functions and plan for technology changes on campus. Evidence of the work of these committees is found in the minutes from meetings of our recent migration to SIS Plus, upgraded computer equipment in the labs on campus, and updated presentation equipment in high-use classrooms on campus. Technology needs and uses have been noted in strategic planning documents from that time. In the past three years, under the MSCA Contract, Campus Governance has established computer steering committees for both academic and administrative computing.

These various committees have served the campus well, but as the auditor has noted, have not always documented their deliberations, discussions and decisions. In establishing an IT steering committee, the College pledges to record the discussions of these groups to document our thoughts, directions and decision-making for campus IT uses. Also, the steering committee will serve as the focal point for the creation of the policies needed to comply with the various auditor recommendations.

Auditor's Reply:

We agree with the College's efforts to establish a set of ground rules or policies and, where applicable, standard procedures to address IT management and operations throughout the College. We believe that IT management and control can be strengthened and made easier by viewing the College as a single enterprise to which IT-related policies and procedures would be applied. In that light, the College would benefit from establishing a framework of internal control policies, standards and practices to be applied across the enterprise as a whole. We also agree with the College's efforts to reestablish IT steering committee oversight.